

Attorney Docket No.: 06975-200001

Client Docket No.: Security 13

APPLICATION FOR UNITED STATES PATENT

in the name of

Robert Hirsh

of

America Online, Inc.

for

**Leveraging a Persistent Connection to
Access a Secured Service**

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Tel.: (202) 783-5070
Fax: (202) 783-2331

ATTORNEY DOCKET:

06975-200001

Leveraging a Persistent Connection to Access a Secured Service

This application claims priority from U.S. Provisional Application No. 60/282,857, titled "One-time Authentication to Gain Access to Multiple Secured Computer Systems" and filed April 11, 2001, which is incorporated by reference in its entirety.

TECHNICAL FIELD

5 This invention relates to providing access to a secured service.

BACKGROUND

10 A secured service may require the provision of authentication information before allowing a connection to be established from a client seeking access. Various secured services may be accessed simultaneously by one client, each generally requiring the accessing client to provide authentication information that is duplicative or additional to the authentication information provided to the other secured services before allowing access to be established. For instance, a client may establish a connection with a first secured service by providing the first secured service with first authentication information. Thereafter, the same client seeking access to other secured services may be required again to provide those other secured services with second authentication information that is duplicative and/or additional to the first authentication information provided to the first secured service.

SUMMARY

20 In one general aspect, leveraging a persistent connection to provide a client access to a secured service includes establishing a persistent connection with the client in response to a first request from the client, and brokering a connection between the client and a secured service based on a second request from the client by leveraging the persistent connection with the client. The brokering may occur before the client attempts to connect to the secured service directly and the connection may be established between the client and the secured service without provision by the client of authentication information duplicative or additional to authentication information provided by the client to establish the persistent connection.

25

Implementations may include one or more of the following features. For example, establishing the persistent connection may include receiving keystone authentication information from the client, authenticating the client based on the keystone authentication information to provide a keystone authentication, and establishing the persistent connection with the client based on the keystone authentication.

Leveraging the persistent connection may include receiving the second request from the client for connection to the secured service after the persistent connection to the client is established. Leveraging the persistent connection also may include providing a leveraged authentication that may be used to establish the connection with the secured service and that is based on the keystone authentication associated with the persistent connection. The keystone authentication also may be used to provide the leveraged authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

The persistent connection may be established between the client and a persistent connection service while the connection between the client and the secured service may be brokered by a broker service. The broker service may receive from the persistent connection service at a connection request address a communication based on the second request from the client, and the persistent connection service may authenticate the client to the broker service by leveraging the persistent connection.

Brokering the connection to the secured service may include communicating as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service. For example, in one implementation brokering includes determining the authorization information based on the second request from the client, and communicating to the secured service an indication that the client desires to connect to the secured service, in which the indication includes the authorization information. A response is received from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service, and the authorization information is communicated to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

In another implementation, brokering includes communicating to the secured service an indication that the client desires to connect to the secured service, receiving a response from the secured service indicating that the secured service may accept a connection from the client, in which the response includes the authorization information, and communicating the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service. The authorization information may be determined by the secured service.

The authorization information may be ineffective to establish a connection with the secured service if the connection constraints are not satisfied by the constraint information. The connection constraints may include, for example, a constraint to limit the number of uses for the authorization information to a predetermined number (e.g., a one-time-use password), and/or information indicating a number of uses to which the authorization information has been put. The connection constraints also may include a constraint that the authorization information be used within a predetermined time window, and/or a constraint that the authorization information be presented to the secured service by a client for whom the connection was brokered.

These general and specific aspects may be implemented using a method, a system, or a computer program, or any combination of systems, methods, and computer programs.

Other features will be apparent from the description, the drawings, and the claims.

DESCRIPTION OF DRAWINGS

Fig. 1 is a schematic diagram of a system configured to provide a client having an established persistent connection with access to a secured service.

Fig. 2 is a schematic diagram illustrating a system, as in Fig. 1, in which the secured service is an IMAP mail service.

Fig. 3 is a schematic diagram illustrating a system, as in Fig. 1, in which the secured service is a synchronization service.

Fig. 4 is a schematic flow diagram illustrating a systematic process implementable by the system of Fig. 1 for providing a client having an established persistent connection with access to a secured service.

Fig. 5 is a schematic flow diagram illustrating a connection process that may be used to establish a persistent connection, as provided generally in Fig. 4.

Figs. 6 and 7 are schematic flow diagrams illustrating processes that may be used to broker a connection with a secured service, as provided generally in Fig. 4.

Fig. 8 is a schematic flow diagram illustrating a process that may be used to establish the brokered connection with the secured service, as provided generally in Fig. 4.

Like reference symbols in the various drawings may indicate like elements.

DETAILED DESCRIPTION

For illustrative purposes, a process is described for leveraging a persistent connection to provide access to a secured service, and systems and software for implementing the process also are described. For clarity of exposition, the description generally proceeds from an account of general elements and their high level relationship to a detailed account of illustrative roles, configurations, and components of the elements.

Referring to Fig. 1, a generalized system 100 may be used to permit a client 110 to leverage a persistent connection 101 to a persistent connection service 130 by which access may be gained to a secured service 170, in which gaining access to the secured service 170 may or may not include establishing another persistent connection with the secured service 170. Exemplary components of the system 100 are described in greater detail below.

The system 100 of Fig. 1 generally includes the client 110, the persistent connection service 130, a broker service 150, and one or more secured services 170.

The client 110 generally may include any device, system, and/or piece of code that relies on another service to perform an operation. For example, the client 110 may include a Web browser, an email client, a synchronization client (e.g., a calendar synchronization client, a task list synchronization client), an instant messaging (IM) client, a software productivity application (e.g., a word processor, a spreadsheet), and/or an operating system or operating system kernel. The client 110 also may be configured to access data that may be stored, for example, in a magnetic and/or an optical storage medium and/or any other acceptable storage medium accessible to the client 110 (e.g., storage medium 111).

The persistent connection service 130 may include, for example, an IM service, an email service (e.g., an IMAP service), a login service, an authentication service, an

authorization service, and/or any other service or combination of services configured to provide a persistent connection, while the broker service 150 may include, for example, any device, system, and/or piece of code configured to broker a connection as hereinafter described between a client with a persistent connection and a secured service.

5 A secured service 170 generally may include, for example, any device, system, and/or piece of code configured to perform an operation requested by a client 110 (e.g., a Web browser, another service). For example, the secured service 170 may include an email service, a synchronization service (e.g., a calendar synchronization service, a task list synchronization service), a print service, a file access service, an IM service, an operating
10 system, an operating system kernel, an authentication service, an authorization service, and/or any combination of these services. The secured service 170 also may include a persistent connection service.

One or more other services may be included in the components of system 100 and/or these components (hereinafter the system services) may be included as part of one or more
15 other services. For example, the system services may include or be included in a general-purpose or a special-purpose computer (e.g., a personal computer, a personal digital assistant (PDAs), or a device specifically programmed to perform certain tasks), at least one Local Area Network (LAN), and/or at least one Wide Area Network (WAN). Either way, the response to and execution of instructions received by any or all of the system services may be
20 controlled by, for example, a program, a piece of code, an instruction, a device, a computer system, or a combination thereof, for independently or collectively instructing the services to interact and operate as described herein.

A persistent connection 101 may be established between the client 110 and the persistent connection service 130 and the persistent connection service 130 may be
25 configured to communicate with the broker service 150, or the broker service 150 may be included as a component of the persistent connection service 130. The broker service 150 and the client 110 may be configured to communicate with the one or more secured services 170.

The persistent connection between the client 110 and the persistent connection
30 service 130 as well as other communications between the system services generally occur over a communications network. The communication network typically allows direct or

indirect communication between the system services (e.g., between the client 110, the persistent connection service 130, the broker service 150, and/or the secured services 170), irrespective of physical or logical separation. The communication network may include a secured communication network (e.g., a communication network protected by a firewall) that may include communication paths 151 and 153 over which the broker service 150 may communicate with the persistent connection service 130 and/or the secured services 170, respectively. The secured communication network, for example, may isolate the broker service 150 from the client 110 so that the broker service 150 is not visible to the client 110.

The communication network may include various mechanisms for delivering voice and/or non-voice data, such as, for example, the transport connection protocol (TCP), the Internet protocol (IP), the World Wide Web, one or more local area networks (LANs) and/or one or more wide area networks (WANs). The communication network also may include analog or digital wired and wireless telephone networks, e.g., public switched telephone networks (PSTN), integrated services digital networks (ISDN), various types of digital subscriber lines (xDSL), advance mobile telephone service (AMPS), global system for mobile communications (GSM), code division multiple access (CDMA), radio, cable, satellite, and/or other delivery mechanisms for carrying voice or non-voice data.

To communicate voice and/or non-voice data, the system services may include one or more communications systems in addition to the components described above, such as, for example, an analog, a digital, or a cellular telephone, whether wired or wireless, a program, a piece of code, an instruction, a device, a computer, a computer system, or a combination thereof, for independently or collectively sending or receiving communications.

Implementations of communications systems may exist permanently or temporarily in any type of machine, component, physical or virtual equipment, storage medium, or propagated signal capable of sending or receiving voice communications.

Figs. 2 and 3 describe systems generally similar to system 100 of Fig. 1 but that illustrate the inclusion of specific secured services (i.e., an email service and a synchronization service, respectively) that may be accessed by the client 110.

Referring to Fig. 2, a system 200 is illustrated in which the client 110 and the broker service 150 may communicate with a secured service 170 that includes an email service 210. The email service 210 may be used to transmit and to receive electronic messages and may

include a mailbox 211 in which received messages may be stored. The email service 210 also may include a mail transfer protocol service 213 that may be used to send an electronic message, using a protocol such as, for example, the simple mail transfer protocol (SMTP). The email service 210 also may include a retrieval service used to retrieve email messages
5 from the mailbox 211 under a protocol, such as, for example, the Internet message access protocol (IMAP), and/or the post office protocol (POP) 215.

Referring to Fig. 3, a system 300 is illustrated in which the client 110 is configured to access data A' (e.g., a modified calendar, a modified task list) that may, for example, include a modified version of original data A (e.g., an original calendar, an original task list). Data
10 A' may be stored, for example, in a magnetic and/or an optical storage medium and/or any other acceptable storage medium accessible to the client 110 (e.g., storage medium 111), whether internal or external to the client 110. The client 110 and the broker service 150 may communicate with a secured service 170 that includes a synchronization service 310 (e.g., the calendar synchronization service or the task list synchronization service mentioned above). The synchronization service 310 may include a sync service 311 that may be configured, for
15 example, to access original data A and to synchronize that original data A with modified data A'. Data A may be stored, for example, in a disk array (e.g., disk array 313) and/or any other acceptable storage medium accessible to the sync service 311, whether internal or external to the sync service 311.

Fig. 4 illustrates a systematic process 400 that may be implement by the system of Fig. 1 to provide a client 110 having an established persistent connection 101 with access to a secured service 170. Process 400 provides that the client 110 may establish a persistent
20 connection 101 with the persistent connection service 130 and the persistent connection service 130 may authenticate the client 110 (hereinafter referred to as keystone authentication) based on authentication information provided by the client 110 (step 411). The persistent connection service 130 may or may not include the broker service 150.

Later, after the persistent connection 101 is established, the client 110 may request access to a desired secured service 170 (step 413). For example, the client 110 may request the connection to the secured service 170 by sending the request for that access to the
30 persistent connection service 130.

When embodied separately from the broker service, the persistent connection service 130 typically forwards the connection request to the broker service 150 at a connection request address associated with the broker service 150. The persistent connection service 130 may leverage the keystone authentication to authenticate the client 110 to the broker service 150, without requiring the client 110 to provide duplicative or additional authentication information.

Following receipt of the connection request, the broker service 150 may search for and determine an acceptable secured service 170 (e.g., an email service if the client 110 wishes to send or receive an electronic message) (step 420) and may broker a connection with the secured service 170 (examples of brokering are described in detail with respect to Figs. 6 and 7) (step 431). Authorization information (described in greater detail below) may be determined during the brokering of the connection (step 431) and the keystone authentication may be leveraged to authenticate the client 110 to the secured service 170.

If the broker service 150 is unable to broker a connection with the determined secured service 170 (step 433), then the broker service 150 may perform a recovery procedure (step 440). The recovery procedure (step 440) may include determining whether it is appropriate to retry brokering with the secured service 170 (e.g., a retry may occur where brokering has failed less than a predetermined threshold of times) (step 441), and, if determined appropriate, the broker service 150 may attempt again to broker a connection with the secured service 170 (step 431). Otherwise, the broker service 150 may determine whether to search for another secured service 170 with which to broker a connection (e.g., another secured service 170 may be sought where less than a predetermined threshold of time has elapsed since the client 110 requested access to a secured service 170) (step 443). If determined appropriate, the broker service 150 may search for a different secured service 170 (step 420), or, if not, the broker service 150 may communicate to the client 110 a failure successfully to broker a connection with a secured service 170 (step 445) after which the client may or may not request the broker service to broker another connection (step 413).

If, however, the broker service 150 successfully brokered a connection to the secured service 170 (step 433), then the broker service 150 may provide the authorization information determined during the brokering process to the client 110 (step 435). The authorization information may be used by the client 110 to contact the secured service 170. The secured

service 170 may receive the authorization information and may determine if the authorization information satisfies one or more connection constraints (examples of constraints are described below and with respect to Fig. 8) (step 453).

If the connection constraints are not satisfied (step 453), then the secured service 170 may not accept the authorization information and may refuse the connection. Upon refusal of the connection by the secured service 170, the client 110 may determine whether it is appropriate to retry connecting using the authorization information (step 460). For instance, it may be appropriate to retry where the authorization information has been refused less than a predetermined number of times and/or where the connection constraints associated with the authorization information are not known to be violated. If determined appropriate, the client 110 may again provide the authorization information to the secured service 170 (step 451). Otherwise, the client 110 may or may not receive a report of the failed connection (step 470) and/or request that the broker service 150 broker a connection with another secured service 170 (step 413).

By contrast, if the secured service 170 determines that the authorization information satisfies the connection constraints (step 453), then the secured service 170 may accept the authorization information and may permit the client 110 to connect to the secured service 170 (step 455).

The connection constraints, mentioned above with respect to step 453, may include, for example, a constraint that the authorization information has been used (e.g., received by the secured service 170 and/or accepted by the secured service 170) no more than a predetermined number of times (e.g., once), a constraint that the authorization information should be used within a predetermined time window (e.g., thirty-seconds from the time of determination of the authorization information), and/or a constraint that the authorization information be received from the same client 110 for whom the connection was brokered.

The authorization information may include constraint information that may be used to determine if the authorization information satisfies the connection constraints. Moreover, the authorization information may include a password and the password may include some or all of the constraint information. The constraint information may include an indication of a number of uses for which the authorization information may be considered valid (e.g., 1, 2, 3), an indication of a time when the authorization information was determined (e.g., a time

stamp), and/or an indication of a window of time relative to the time stamp during which the authorization information may be considered valid. The constraint information also may include information indicative of an identity of the client 110 for whom the authorization information was determined.

5 For example, the password may include constraint information, such as, a screen name, a login name, a biometric signature, and/or a digital signature of the client 110, or any combination of these. The password also may contain constraint information indicating that the password is valid for only one use, is valid only if used within thirty-seconds of determination of the password, and/or is valid only if received from the client 110 for whom
10 the password was determined (e.g., a one-time use, time-limited, designated-user password, hereinafter a constrained password).

Fig. 5 illustrates a process 410 by which the client 110 may establish a persistent connection 101 and may request a connection to a secured service 170, and that may be used in one implementation of the process of Fig. 4. The process 410 includes establishing a persistent connection 101 between the client 110 and a persistent connection service 130
15 (step 505). Before allowing the client 110 to establish the persistent connection 101, the persistent connection service 130 may require that the client 110 provide authentication information by which the persistent connection service 130 may authenticate the client 110 (the keystone authentication). Thereafter, the client 110 may communicate a request to the persistent connection service 130 to connect to a secured service 170, which request may
20 include information indicating a secured service 170 to which connection is desired (step 510). The persistent connection service 130 may forward the connection request to the broker service 150 (step 515) and also may leverage the keystone authentication to authenticate the client 110 to the broker service 150, e.g., without provision of duplicative or
25 additional authentication information by the client 110.

Fig. 6 illustrates an exemplary implementation of the process 430 of Fig. 4 that may be used to broker a connection to the secured service 170. As illustrated by Fig. 6, the broker service 150 may authenticate the client 110 based on the persistent connection 101 of the client 110 to the persistent connection service 130 (e.g., by leveraging the keystone authentication) (step 605). The broker service 150 then may generate/determine a
30 constrained password (step 610) and also may generate a request-to-honor for the constrained

password that may include the constrained password (step 615). The broker service 150 may submit the request-to-honor to the secured service 170 and may leverage the persistent connection 101 of the client 110 to authenticate the client 110 to the secured service 170 (step 620). The secured service 170 may reject the request-to-honor (step 625), which may cause the broker service 150 to perform a recovery procedure (step 630) that generally may be similar to recovery procedure 440 of Fig. 4. Otherwise, if the request to honor is accepted by the secured service 170 (step 625), then the secured service 170 may store the constrained password and reply to the broker service 150 with a target connection point (step 635), such as, for example, an IP address, a World Wide Web address, a port, a socket, and/or any combination of these. The broker service 150 may communicate the target connection point and the constrained password to the client 110 (e.g., by communicating the target connection point and the constrained password to the persistent connection service 130 to forward to the client 110) (step 640).

Fig. 7 illustrates another process 430 that may be used to broker a connection to the secured service 170 and to implement the process of Fig. 4. The broker service 150 may authenticate the client 110 based on the persistent connection 101 of the client 110 to the persistent connection service 130 (e.g., by leveraging the keystone authentication) (step 705). The broker service 150 then may generate a connection authorization request (step 710) and may submit the connection authorization request to the secured service 170 while leveraging the persistent connection 101 of the client 110 to authenticate the client 110 to the secured service 170 (step 715). The secured service 170 may reject the connection authorization request (step 720), which may cause the broker service 150 to perform a recovery procedure (step 725) that generally may be similar to recovery procedure 440 of Fig. 4. Otherwise, if the connection authorization request is accepted by the secured service 170 (step 720), then the secured service 170 may reply to the authorization request by providing to the broker service 150 a constrained password and/or a target connection point that the secured service 170 also may retain and store (step 730). The broker service 150 may communicate the target connection point and the constrained password to the client 110 (e.g., by communicating the target connection point and the constrained password to the persistent connection service 130 to forward to the client 110) (step 735).

Fig. 8 illustrates a process for establishing a connection to the secured system by presenting the constrained password to the secured system that may be used in one implementation of the process of Fig. 4. The client 110 may present the constrained password to the secured service 170 at the connection point (step 805) and the secured service 170 may receive the constrained password at the connection point (step 810). Thereafter, the secured service 170 may determine if the constrained password satisfies the connection constraints, such as, for example, a constraint that the constrained password match the constrained password previously stored, that the constrained password has not previously been presented and/or used (e.g., the constrained password may be a one-time use password), that the constrained password is presented within an acceptable time window (e.g., the constrained password may be a time limited password) (step 810). The secured service 170 may refuse the connection if the constrained password does not satisfy the connection constraints, and the client 110 then may execute a retry procedure (step 815) that may correspond generally to step 460 of the process of Fig. 4. Otherwise, if the constrained password does satisfy the connection constraints (step 810), then the secured service 170 may allow the connection to be established (step 820).

Other implementations are within the scope of the following claims.